UNITED STATES PATENT AND TRADEMARK OFFICE

A

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/819,359	03/28/2001	Satoshi Hada	JP919990280US1	3306

23389 7590 11/15/2005

SCULLY SCOTT MURPHY & PRESSER, PC
400 GARDEN CITY PLAZA
SUITE 300
GARDEN CITY, NY 11530

EXAMINER	
POLTORAK, PIOTR	

ART UNIT	PAPER NUMBER
2134	

DATE MAILED: 11/15/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Advisory Action Before the Filing of an Appeal Brief	**Application No.** 09/819,359	**Applicant(s)** HADA, SATOSHI	
	Examiner Peter Poltorak	**Art Unit** 2134	

--The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

THE REPLY FILED 17 October 2005 FAILS TO PLACE THIS APPLICATION IN CONDITION FOR ALLOWANCE.

1. ☐ The reply was filed after a final rejection, but prior to or on the same day as filing a Notice of Appeal. To avoid abandonment of this application, applicant must timely file one of the following replies: (1) an amendment, affidavit, or other evidence, which places the application in condition for allowance; (2) a Notice of Appeal (with appeal fee) in compliance with 37 CFR 41.31; or (3) a Request for Continued Examination (RCE) in compliance with 37 CFR 1.114. The reply must be filed within one of the following time periods:
   a) ☐ The period for reply expires _____months from the mailing date of the final rejection.
   b) ☒ The period for reply expires on: (1) the mailing date of this Advisory Action, or (2) the date set forth in the final rejection, whichever is later. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of the final rejection.

   Examiner Note: If box 1 is checked, check either box (a) or (b). ONLY CHECK BOX (b) WHEN THE FIRST REPLY WAS FILED WITHIN TWO MONTHS OF THE FINAL REJECTION. See MPEP 706.07(f).

Extensions of time may be obtained under 37 CFR 1.136(a). The date on which the petition under 37 CFR 1.136(a) and the appropriate extension fee have been filed is the date for purposes of determining the period of extension and the corresponding amount of the fee. The appropriate extension fee under 37 CFR 1.17(a) is calculated from: (1) the expiration date of the shortened statutory period for reply originally set in the final Office action; or (2) as set forth in (b) above, if checked. Any reply received by the Office later than three months after the mailing date of the final rejection, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

NOTICE OF APPEAL

2. ☐ The Notice of Appeal was filed on _____. A brief in compliance with 37 CFR 41.37 must be filed within two months of the date of filing the Notice of Appeal (37 CFR 41.37(a)), or any extension thereof (37 CFR 41.37(e)), to avoid dismissal of the appeal. Since a Notice of Appeal has been filed, any reply must be filed within the time period set forth in 37 CFR 41.37(a).

AMENDMENTS

3. ☐ The proposed amendment(s) filed after a final rejection, but prior to the date of filing a brief, will not be entered because
   (a) ☐ They raise new issues that would require further consideration and/or search (see NOTE below);
   (b) ☐ They raise the issue of new matter (see NOTE below);
   (c) ☐ They are not deemed to place the application in better form for appeal by materially reducing or simplifying the issues for appeal; and/or
   (d) ☐ They present additional claims without canceling a corresponding number of finally rejected claims.

   NOTE: _____. (See 37 CFR 1.116 and 41.33(a)).
4. ☐ The amendments are not in compliance with 37 CFR 1.121. See attached Notice of Non-Compliant Amendment (PTOL-324).
5. ☐ Applicant's reply has overcome the following rejection(s): _____.
6. ☐ Newly proposed or amended claim(s) _____ would be allowable if submitted in a separate, timely filed amendment canceling the non-allowable claim(s).
7. ☐ For purposes of appeal, the proposed amendment(s): a) ☐ will not be entered, or b) ☐ will be entered and an explanation of how the new or amended claims would be rejected is provided below or appended.
   The status of the claim(s) is (or will be) as follows:
   Claim(s) allowed: _____.
   Claim(s) objected to: _____.
   Claim(s) rejected: _____.
   Claim(s) withdrawn from consideration: _____.

AFFIDAVIT OR OTHER EVIDENCE

8. ☐ The affidavit or other evidence filed after a final action, but before or on the date of filing a Notice of Appeal will not be entered because applicant failed to provide a showing of good and sufficient reasons why the affidavit or other evidence is necessary and was not earlier presented. See 37 CFR 1.116(e).
9. ☐ The affidavit or other evidence filed after the date of filing a Notice of Appeal, but prior to the date of filing a brief, will not be entered because the affidavit or other evidence failed to overcome all rejections under appeal and/or appellant fails to provide a showing a good and sufficient reasons why it is necessary and was not earlier presented. See 37 CFR 41.33(d)(1).
10. ☐ The affidavit or other evidence is entered. An explanation of the status of the claims after entry is below or attached.

REQUEST FOR RECONSIDERATION/OTHER

11. ☒ The request for reconsideration has been considered but does NOT place the application in condition for allowance because: See Continuation Sheet.
12. ☐ Note the attached Information Disclosure Statement(s). (PTO/SB/08 or PTO-1449) Paper No(s). _____
13. ☐ Other: _____.

Continuation of 11. does NOT place the application in condition for allowance because: There appears to be some confusion regarding the previous rejection. In an attempt to elucidate the rejection the examiner provides additional clarification addressing applicant's remarks.

Applicant argues that applicant's invention requires 5 "cryptograms" A, B, X, C, Y and X and Schneier teaches only two: x and y.
The examiner points out that in discussion on Diffie-Helman Schneier teaches X (corresponding to applicant's A), Y (corresponding to B) and k' (corresponding to X) (Schneier, pg. 513).
As presented in the previous Office Action it would have been obvious to one of ordinary skill in the art at the time of applicant's invention to enhance Diffie-Helman's method given the benefit of mutual authentication.
The authentication suggested by Schneier in view of Trostle (as presented in the previous Office Action) is nothing else but a (cryptographic) challenge response transaction, since in challenge response transactions a first party sends a value to a second party that operates on the value producing other values. Other values are sent back to the first party using the values to authenticate the second party.
In mutual authentication parties take turns in authenticating each other and thus the mutual authentication that utilizes challenge response techniques will simply result in the challenge response initiated by the first party followed by the challenge response initiated by the second party.
In Schneier in view of Trostle, the challenge response is first initiated by p (the first party) that creates and sends X to v (the second party). Using X, v creates and returns values B and X that are verified by p to authenticate v (to verify that X=F(B,a)).
As discussed above, in MUTUAL authentication the challenge response will be followed by the transaction initiated by the second party. Since, in the instant case v has already created B and X that has been sent to p for benefit of speed it would have been obvious to use one of these values.
Thus the step of creating and sending the value B to p that results in creation of C and Y that is sent back to p that based on these value authenticates, v is essentially the repeat of the authentication steps (although using different values) but this time is initiated by the other (second) party.
Thus, Schneier in view of Trostle do teach 5 "cryptograms" A; B, X, C, Y and the specifics that are recited in the claim language.

As per Diffie Helman's key exchange, applicant argues Schneier's disclosure as presented in the previous Office Action and concludes that neither of the cryptograms X and Y include a secret key, nor do the computations respectively carried out by the engaged parties verify the relation between a public key v and a secret key s.
The examiner points out that although no explicit teaching to applicant's v=F(g,-s) (recited in the preamble) has been provided in the previous Office Action it is inherent that in the public/private encryption (as implemented by Diffie Helman for example) there must be a relationship such that if there is a "v" corresponding to a public or private key there must be an "s" (corresponding to private or public key) such that v=F(g, -s). In public cryptography in order to decrypt encrypted information the corresponding (inverse) decryption key is required.
Furthermore, in the previous Office Action the examiner did not claim that Diffie Helman's algorithm as presented by Schneier was used for authentication. However, as discussed above Diffie Helman's algorithm corresponds to applicant's invention (§ 13).
Lastly, as cited by the examiner, Schnorr teaches an authentication protocol that checks whether A=J(v, Y, g, Z). The cipher, impersonation and spoofing attacks are well known in the art of computer security and it would have been obvious to one of ordinary skill in the art at the time of applicant's invention to implement an additional verification such as Schnorr's that verifies the prover given the benefit of an increased level of security.

GREGORY MORSE
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER